(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 January 2003 (30.01.2003)

PCT

(10) International Publication Number
WO 03/009285 A2

(51) International Patent Classification⁷: G11B 20/00

(21) International Application Number: PCT/IB02/02548

(22) International Filing Date: 25 June 2002 (25.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01202770.2 19 July 2001 (19.07.2001) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: KAMPERMAN, Franciscus, L., A., J.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). LINNARTZ, Johan, P., M., G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: DEGUELLE, Wilhelmus, H., G.; International Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

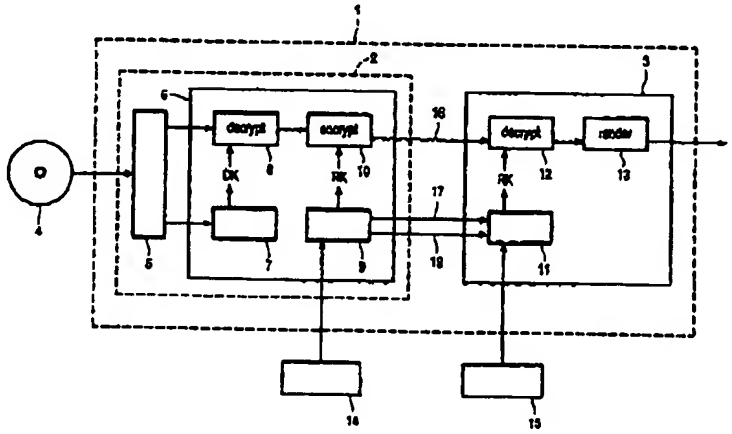
(81) Designated States *(national)*: CN, IN, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR REPRODUCING USER DATA



(57) Abstract: The invention relates to an apparatus and a method for reproducing user data stored in encrypted form on a recording medium. In order to provide a higher level of protection against hacking of user data and, in particular, of decryption keys, which are used for encrypting said user data and which are also stored on the recording medium, an apparatus is proposed according to the invention, comprising:- means for reading user data and key data from said recording medium, - an integrated unit including- means for calculating a decryption key using said key data, - means for decrypting user data read from said recording medium using said calculated decryption key, and - means for re-encrypting said decrypted data using a re-encryption key,- means for transmitting said re-encrypted data from said integrated unit to an application unit, and- an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

WO 03/009285 A2

Apparatus and method for reproducing user data

The invention relates to an apparatus and a method for reproducing user data stored in encrypted form on a recording medium as well as to an integrated circuit for use in such an apparatus or method. The invention refers particularly to the protection of information stored on removable recording media, such as video data on a DVD.

If user data, e. g. video data, audio data, software or application data, is stored on a removable recording medium in encrypted form it is most often required that an authorized application can read and use said user data, if allowed, from such removable recording media without the need to retrieve the decryption key from a separate location such as the internet. Hence, the decryption key has to be stored on the medium together with the encrypted user data.

However, the decryption key has to be hidden from an unauthorized access. Known techniques for hiding the decryption key are the use of a media-key-block with secrete player keys which are, for instance, used in the known Content Scrambling System (CSS) and in Content Protection for Recordable Media (CPRM). Another method for hiding the decryption key in electronic signals using secret signal processing methods is known from US 6,157,606. Therein a master key is used for encrypting main data in a pit-width direction by changing a light amount of a laser beam to then record it on an optical recording medium.

In the current protection systems, such as CSS and CPRM, the calculation of the decryption key is performed inside an authorized PC application running in an application unit of a PC. These authorized applications contain protection mechanisms against the extraction of secrets, such as player keys needed for media-key-block calculation, and against any modification of the behaviour of the application, such as providing any protected data in the clear to other applications. These protection mechanisms for PC software applications are, however, known to be weak and to fail regularly. If the authorized application and/or the application unit is tampered with by hackers, it could be changed such that it provides the hacker with the decryption key of the protected user data. The hacker would now be able to

extract and publish the decryption keys of many published recording media which would allow other hackers to get easy access to the protected user data using unauthorized applications.

This is a serious security problem. The illegal distribution of decryption keys does potentially produce more damage than the illegal distribution of protected user data in the clear because the protected user data includes a large amount of data, usually many megabytes, and is therefore time-consuming. In contrast, the decryption keys include only a small amount of data, usually not much more than one kilobyte, and can be distributed quickly and widely.

It is therefore an object of the present invention to provide an apparatus and a method for reproducing user data stored in encrypted form on a recording medium which provide a higher level of protection, in particular of the decryption key, against theft through hacking of a PC application and/or application unit. This object is achieved by providing an apparatus as claimed in claim 1, comprising:

- means for reading user data and key data from said recording medium,
- an integrated unit including
  - means for calculating a decryption key using said key data,
  - means for decrypting user data read from said recording medium using said calculated decryption key, and
  - means for re-encrypting said decrypted data using a re-encryption key,
- means for transmitting said re-encrypted data from said integrated unit to an application unit, and
- an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

This object is further achieved by a corresponding method as claimed in claim 8. An integrated unit for use in such an apparatus for use in such a method is claimed in claim 9 comprises:

- means for calculating a decryption key using key data read from said recording medium,
- means for decrypting user data read from said recording medium using said calculated decryption key, and
- means for re-encrypting said decrypted data using a re-encryption key to obtain re-encrypted data for being transmitted to an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

The present invention is based on the idea to decrypt and to re-encrypt the user data read from the recording medium inside an integrated unit in the drive and not, as usually, inside an application unit using a PC application. Such an integrated unit is much more difficult to hack compared to an application unit, and thus provides an improved protection for the decryption key. In addition, the calculation of the decryption key used for decrypting the user data and the calculation of a re-encryption key used for re-encrypting the decrypted user data are also performed inside the integrated unit which even more improves protection of the decryption key. The decryption key thus never leaves the integrated unit, neither in encrypted form nor in decrypted form. Further, the decrypted user data that exists between decryption and re-encryption is never visible outside the integrated unit which also provides a higher level protection against hacking of user data.

In order to enable the application unit to decrypt and then to reproduce the user data provided from the integrated unit to the application unit the re-encryption key or any data for calculating the re-encryption key needs to be provided to the application unit. This can be done by different methods, e. g. using public key cryptography or by transmitting the re-encryption key over a secure authenticated channel (SAC) from the integrated unit to the application unit. Alternatively, also a symmetric cryptographic method can be used for this purpose.

Preferred embodiments of the invention are included in the dependent claims. It shall be understood that the apparatus as claimed in claim 1, the method as claimed in claim 7 and the integrated circuit as claimed in claim 8 can be developed further and can have identical or similar embodiments.

Preferably, said integrated unit is included in a drive unit for reading recording media and said drive unit as well as said application unit are included in a computer like a PC. It is further preferred that the recording medium is an optical recording medium, in particular a disc, which may be recordable or rewriteable and which is preferably a CD or a DVD storing any kind of user data. Alternatively, the recording medium may also be another, comparable medium, e.g. a solid state memory card.

In a still further preferred embodiment the integrated unit is realized as an integrated circuit which can not easily be hacked from outside. However, said integrated unit may also be understood as another integrated component, like e.g. an optical drive unit. If such an integrated component is found to be secure enough re-encryption may be implemented partly in hardware and partly in firmware, e.g. re-encryption key generation may be implemented in firmware. This might be acceptable from a security point of view as

the re-encryption key will also be present in the application unit which is a less secure environment that such an integrated component like an optical drive unit.

The invention will now be explained in more detail with reference to the figure which shows a block diagram of a reproducing apparatus according to the invention.

Therein a personal computer 1 is shown comprising a drive unit 2 and an application unit 3. If a user intends to reproduce user data stored on a recording medium 4 like a DVD-ROM, e. g. to replay video data stored in a DVD in MPEG-format, the medium 4 is inserted into the drive 2 wherein said user data and key data are read by reading means 5. It should be noted that both the user data and the key data are stored on the medium 4 in encrypted form. It should further be noted that there are different ways of encrypting user data and key data for storing it on recording media, but that it is not relevant for the present invention which particular way is used.

The read data are then input into an integrated unit 6, which is preferably realized by an integrated circuit (IC) comprising different means for calculating keys and for decrypting and re-encrypting user data. At first the decryption key is calculated in a key calculation unit 7 using the read key data inputted from the reading means 5. This decryption key DK is required for decrypting the read user data inputted from the reading means 5 to the decryption unit 8. This decryption key DK is identical to an encryption key which has been used for encrypting the user data before storing it on the medium 4 or is a corresponding key to this encryption key.

After decryption the user data shall be re-encrypted in a re-encryption unit 10 instead of outputting the user data in the clear over a bus 16 directly to the application unit 3 since such a transmission of user data in the clear over a bus is not very secure and gives hackers an opportunity to read and copy the user data.

The re-encryption key RK used for re-encrypting the user data is also calculated inside the integrated unit 6 by an appropriate key calculation unit 9. Since this re-encryption key RK has also to be known to the application unit 3 in order to decrypt the user data therein, a secure authenticated channel 17, 18 between the drive unit 2 and the application unit 3 is established. To authorize the application running on the application unit 3 its public key is certified by a certification authority 15.

If the application is thus authorized a corresponding indication thereof, in particular a public key of the application is transmitted from the application unit 3 to the drive 2, in particular, to the key calculation unit 9 of the integrated unit 6. The key calculation unit 9 may then authorize the application by checking the certificate of the public key application with a public key licensing authority 14 and by checking if the application possesses the corresponding private key which is part of the SAC functionality.

After final authorization of the application the encrypted re-encryption key RK or any other data relating to the re-encryption key are transmitted from the key calculation unit 9 to the key calculation unit 11 of the application unit 3 via transmission line 18. The key calculation unit 11 is thus able to calculate the re-encryption key RK such that the decryption unit 12 can decrypt the re-encrypted user data provided via transmission line 16. It should be noted that the transmission lines 16, 17 and 18 are included in the PC bus of the computer 1.

After decrypting the user data in decryption unit 12 it can be completely reproduced and rendered for playback by render unit 13.

The invention thus provides a high level of protection against theft of user data and/or of decryption keys used for encrypting the user data before storing it on the recording medium. Neither the user data nor the decryption keys are transmitted over a bus of the computer or are existent outside of the integrated unit in the clear. It is thus not possible to retrieve the decryption key by hacking the application running on the computer.

CLAIMS:

1. Apparatus for reproducing user data stored in encrypted form on a recording medium, comprising:
- means for reading user data and key data from said recording medium,
- an integrated unit including
  - means for calculating a decryption key using said key data,
  - means for decrypting user data read from said recording medium using said calculated decryption key, and
  - means for re-encrypting said decrypted data using a re-encryption key,
- means for transmitting said re-encrypted data from said integrated unit to an application unit, and
- an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

2. Apparatus according to claim 1, wherein said integrated unit and/or said application unit comprises means for calculating said re-encryption key.

3. Apparatus according to claim 1, further comprising public key cryptography means for exchanging information on said re-encryption key.

4. Apparatus according to claim 3, wherein said public key cryptography means are employed to set up a secure authenticated channel for transmitting said re-encryption key from said integrated unit to said application unit.

5. Apparatus according to claim 1, wherein said integrated unit is included in a drive unit for reading recording media and wherein said drive unit and said application unit are included in a computer.

6. Apparatus according to claim 1, wherein said recording medium is an optical recording medium, in particular a CD or a DVD.

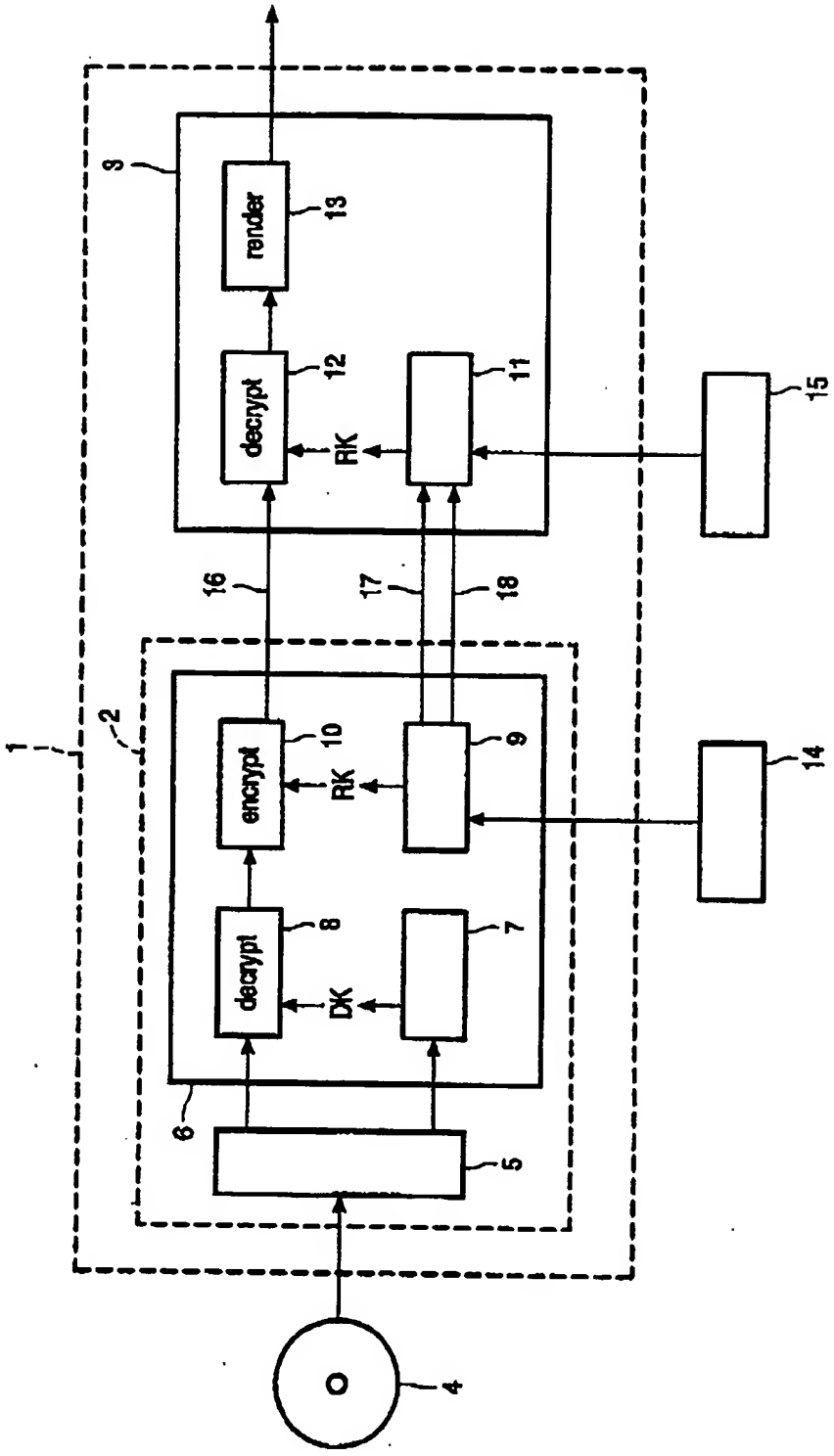
7. Apparatus according to claim 1, wherein said integrated unit is an integrated circuit.

8. Method for reproducing user data stored in encrypted form on a recording medium, comprising the steps of:
- reading user data and key data from said recording medium,
- calculating a decryption key using said key data,
- decrypting user data read from said recording medium using said calculated decryption key,
- re-encrypting said decrypted data using a re-encryption key,
wherein said calculation step, said decryption step and said re-encryption step are carried out in an integrated unit,
- transmitting said re-encrypted data from said integrated unit to an application unit,
- decrypting said re-encrypted data using said re-encryption key in said application unit, and
- reproducing the decrypted data.

9. Integrated unit for use in an apparatus according to claim 1 for reproducing user data stored in encrypted form on a recording medium, comprising:
- means for calculating a decryption key using key data read from said recording medium,
- means for decrypting user data read from said recording medium using said calculated decryption key, and
- means for re-encrypting said decrypted data using a re-encryption key to obtain re-encrypted data for being transmitted to an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

10. Integrated unit according to claim 9, wherein said integrated unit is an integrated circuit.

1/1


render
13
9
decrypt
12
RK
11
15
16
17
18
encrypt
10
RK
9
14
2
1
decrypt
8
DK
7
6
5
O
4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 January 2003 (30.01.2003)

PCT

(10) International Publication Number
WO 03/009285 A3

(51) International Patent Classification[7]: G11B 20/00

(21) International Application Number: PCT/IB02/02548

(22) International Filing Date: 25 June 2002 (25.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01202770.2 19 July 2001 (19.07.2001) EP

(71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors: KAMPERMAN, Franciscus, L., A., J.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). LINNARTZ, Johan, P., M., G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: DEGUELLE, Wilhelmus, H., G.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: CN, IN, JP.

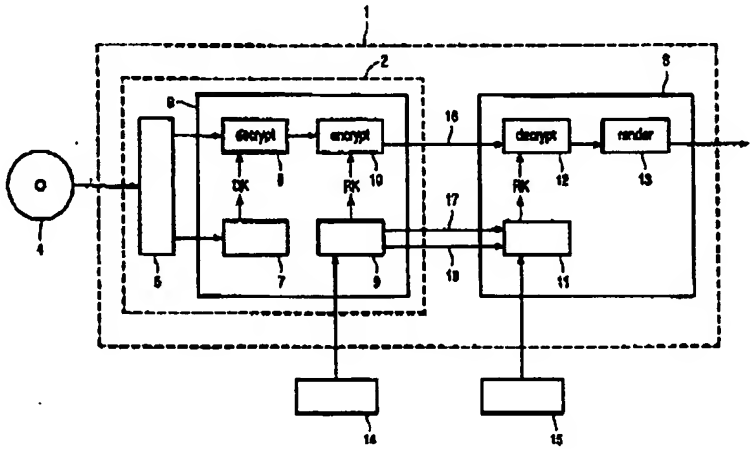
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
5 June 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: APPARATUS AND METHOD FOR REPRODUCING USER DATA



(57) Abstract: The invention relates to an apparatus and a method for reproducing user data stored in encrypted form on a recording medium. In order to provide a higher level of protection against hacking of user data and, in particular, of decryption keys, which are used for encrypting said user data and which are also stored on the recording medium, an apparatus is proposed according to the invention, comprising:- means for reading user data and key data from said recording medium, - an integrated unit including- means for calculating a decryption key using said key data, - means for decrypting user data read from said recording medium using said calculated decryption key, and - means for re-encrypting said decrypted data using a re-encryption key,- means for transmitting said re-encrypted data from said integrated unit to an application unit, and- an application unit for decrypting said re-encrypted data using said re-encryption key and for reproducing the decrypted data.

WO 03/009285 A3

Internat Appacation no
PCT/JP 02/02548

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 978 839 A (HEWLETT PACKARD CO) 9 February 2000 (2000-02-09) * page 3 - page 4 * abstract; figure 1	1-10
A	BRUCE SCHNEIER: "Applied Cryptography Second Edition" 1996 , JOHN WILEY & SONS , USA XP002236172 * page 48 * * page 174 * page 185 -page 187	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 March 2003	09/04/2003

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer
San Millán Maeso, J

Form PCT/ISA/210 (second sheet) (July 1992)

Information on patent family members

PCT/IB 02/02548

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0978839 A	09-02-2000	US 2002016919 A1	07-02-2002
		DE 69902078 D1	14-08-2002
		DE 69902078 T2	07-11-2002
		EP 0978839 A1	09-02-2000
		JP 2000138664 A	16-05-2000

整理番号:　発送番号:166995　発送日:平成21年 3月17日　1

引用非特許文献

特許出願の番号	特願２００４－５６７８１２
作成日	平成２１年　３月　６日
作成者	高橋　克　4538　5S00
発明の名称	暗号化されたアプリケーションをインストールするためのアーキテクチャ